计算机网络安全技术

李巍
liw@buaa.edu.cn

北航计算机学院
2019年春季

网络安全的重要性

- 云计算，物联网的普及，对信息传输、存储、共享的依赖，增加数字世界的风险
- 网络安全已经渗透到国家的政治、经济、社会稳定、军事等领域

安全事件- WannaCry勒索软件

- 2017年5月12日，WannaCry勒索软件
  - 导致100多个国家的数十万用户的计算机遭到攻击，其中包括医疗、教育等公共事业单位和一些大公司
  - 这款恶意代码对计算机内的文档、图片、程序等实施高强度的加密锁定，并向用户索取以比特币支付的赎金。

- 工具：攻击者利用NSA(美国国家安全局)设计的Windows系统黑客工具“永恒之蓝Eternal Blue”
  - 利用Windows的445端口传播，该端口在Windows主要是提供局域网中文件或打印机共享服务。
  - **蠕虫病毒**

安全事件- Mirai僵尸网络

- 物联网Mirai僵尸网络攻击
  - 2016年10月21日，美国多个城市出现互联网瘫痪情况，包括Twitter、Shopify、Reddit等在内的大量互联网知名网站数小时无法正常访问。
  - 美国域名服务提供商Dyn公司遭到大规模的“分布式拒绝访问服务（DDoS）”攻击。

- 工具：Mirai僵尸网络工具，僵尸网络中包含了大量可联网设备
  - 例如监控摄像头、路由器以及智能电视等等。
  - 有大约60万台的物联网设备参与

安全事件-心脏出血Heartbleed漏洞

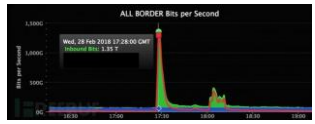
- 开源软件包OpenSSL
  - 提供主要的密码算法、常用的密钥和证书封装管理功能以及SSL协议
- 2014年4月爆出了OpenSSL的Heartbleed漏洞，该漏洞是近年来影响范围最广的高危漏洞，涉及各大网银、门户网站等。
  - 该漏洞可被用于窃取服务器敏感信息，实时抓取用户的账号密码
- OpenSSL又被曝出存在 “水牢DROWN漏洞” （2016年3月）
  - 由于全球2/3的网站服务器都是采用OpenSSL协议加密，为全球网站带来巨大安全挑战。

安全事件-其他

- 中国互联网DNS劫持
  - 2014年1月21日下午3点10分左右，国内通用顶级域的根服务器忽然出现异常，导致众多知名网站出现DNS解析故障，用户无法正常访问。虽然国内访问根服务器很快恢复，但由于DNS缓存问题，部分地区用户“断网”现象仍持续了数个小时，至少有2/3的国内网站受到影响。
- Shellshock破壳漏洞
  - 2014年9月25日，US-CERT公布了一个严重的Bash安全漏洞(CVE-2014 -6271)。由于GNU Bash更广泛的存在，导致其所威胁到的不仅仅是服务器系统，也包括了网络设备、网络交换设备、防火墙等网络安全设备，也包括摄像头、IP电话等很多采用Linux定制的系统。
- IE的0Day漏洞，……

2018年DDOS攻击事件

- 2018年1月，HNS病毒感染逾2万台物联网设备成“肉鸡”
- 2018年1月29日，荷兰三大银行频繁遭受DDoS攻击
- 2018年3月2日，GitHub遭受到严重的DDoS攻击，峰值流量达1.35Tbps
- 2018年4月7日，思科漏洞被黑客利用攻击全球20万台路由器
- 2018年5月底，恶意软件VPNFilter感染超50万台路由器以创建大规模僵尸网络



数据泄露事件

- 雅虎共超15亿用户信息遭窃
- 2.7亿Gmail、雅虎和Hotmail账号遭泄露
- “希拉里邮件门” 事件
- 4.27亿MySpace数据泄漏
- 索尼影业公司被黑客攻击
- iCloud数据泄露
- eBay数据泄露事件
- ……

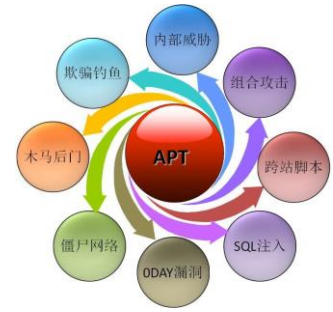
2018年数据泄露事件：

- Facebook数据泄露
- 圆通10亿快递信息泄露
- 喜达屋酒店客房预订数据库遭黑客入侵
- 瑞士数据管理公司 Veeam 泄露 4.45 亿条用户数据
- 问答网站 Quora户数据遭泄露1个亿
- AcFun受黑客攻击，近千万条用户数据外泄
- 加拿大两大银行遭黑客攻击近9万名客户数据被窃

APT攻击事件

- APT攻击(Advanced Persistent Threat，高级持续性威胁)是利用先进的攻击手段对特定目标进行长期持续性网络攻击的攻击形式。
  - 90%以上的APT目标攻击采用**鱼叉式网络钓鱼**攻击手法。
  - 高危漏洞修复率偏低
- 2018年APT攻击事件
  - **韩国平昌冬奥会APT攻击事件**，其导致了奥运会网站的宕机和网络中断。
  - **VPNFilter：针对乌克兰IOT设备的恶意代码攻击事件**，该事件影响了至少全球54个国家和地区的50W设备，包括常用的小型路由器型号(例如Linksys，MikroTik，NETGEAR和TP-Link)、NAS设备等。
  - APT28针对欧洲、北美地区的一系列定向攻击事件
  - 蓝宝菇APT组织针对中国的一系列定向攻击事件
  - 海莲花APT组织针对我国和东南亚地区的定向攻击事件
  - ……

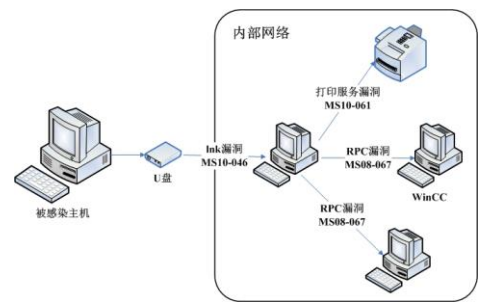
APT的攻击方法



例：震网攻击(超级工厂病毒攻击)

- 2010年伊朗布什尔核电站遭到Stuxnet蠕虫的攻击，导致离心机超速运转并损毁
- 核电站计算机系统实际上是与外界物理隔离的，理论上不会遭遇外界攻击。
- 超级工厂病毒的攻击者针对核电站相关工作人员的家用电脑、个人电脑等能够接触到互联网的计算机发起感染攻击，以此为第一道攻击跳板，进一步感染相关人员的U盘
- 病毒以U盘为桥梁进入“堡垒”内部，利用多种漏洞，包括当时的一个0day漏洞进行破坏。
- 有效控制攻击范围

震网攻击（续）

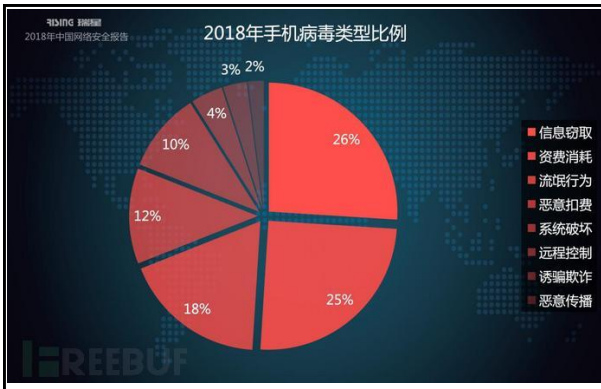


APT攻击受害目标（2018）

来源：360天眼实验室**全球高级持续性威胁（APT）2018年总结报告**
https://www.freebuf.com/articles/paper/193553.html

1	Trojan.Vools!8.F279	通过漏洞传播，窃取敏感信息的木马病毒
2	Backdoor.Agent!8.C5D	使用永恒之蓝攻击工具包，攻击局域网中的计算机，传播挖矿病毒
3	Trojan.Vools!1.B1FA	使用永恒之蓝攻击工具包，攻击局域网中的计算机，传播挖矿病毒
4	Trojan.TaojinStar!8.B91	窃取敏感信息的木马病毒
5	Trojan.Win32/64.XMR-Miner!1.ADCC	挖矿木马
6	Trojan.ShadowBrokers!8.B976	漏洞利用木马病毒
7	Trojan.Agent!8.B1E	具有常见木马行为的一类病毒
8	Trojan.CoinMiner!8.30A	挖矿木马
9	Dropper.Generic!8.35E	病毒释放器，执行后释放病毒文件
10	Downloader.Chindo!8.436	从网络上下载其他木马病毒

来源：瑞星2018年中国网络安全报告，https://www.freebuf.com/articles/paper/194644.html



来源：瑞星2018年中国网络安全报告，https://www.freebuf.com/articles/paper/194644.html

我国网络安全现状

- 2018年8月，互联网络信息中心(CNNIC)今日发布第42次《中国互联网络发展状况统计报告》“第五章 互联网安全管理”
  - 网民上网过程中遇到的安全问题（2018年上半年和2017年对比）

我国网络安全现状

类别	2018年上半年统计数据
境内感染网络病毒终端数	483万个
境内被篡改网站数量	15672个
被植入后门网站数量	16210个
仿冒页面数量	19070个（较2017年同期增长49.1%）
安全漏洞	7748个

注：数据来源：第42次CNNIC报告第五章：互联网安全管理

网络安全的趋势

- 勒索软件成为网络攻击的主要手段之一
  - 传播途径、加密手段多样化
- 物联网设备的安全威胁日趋严重
- 针对关键基础设施的网络攻击升级，攻防两端的对抗将加剧
- 人工智能成为网络安全领域的热点
  - 人工智能将是下一代安全解决方案的核心
- 云、物联网与数字化推动身份认证技术变革
  - 2017年的Verizon数据泄露报告显示，81%的数据泄露都与身份被窃取有关系。如何安全地管理身份验证?
- 培养网络空间安全人才将成为行业热点

网络空间（Cyberspace）

- 网络空间成为人类生活新空间
- 网络空间的基本概念（Cyberspace）
  - 1991年9月号《科学美国人》出版《通信、计算机和网络》专刊，第一次出现“网络空间Cyberspace”
  - 是通过全球互联网和计算系统进行通信、控制和信息共享的动态（不断变化）虚拟空间*
  - 在信息时代是社会有机运行的神经指挥系统，目前已经成为与陆、海、空、太空之后的第五空间。

*《积极构建网络空间安全创新人才培养体系》，http://www.cac.gov.cn/中共中央网络安全和信息化领导小组办公室

网络空间（Cyberspace）组成

- 由独立且互相依存的信息基础设施和网络组成，包括互联网、电信网、计算机系统、嵌入式处理器和控制器系统及其承载的应用
  - 网络互联而成的各种计算系统（包括各种智能终端）
  - 连接端系统的网络
  - 连接网络的互联网和受控系统
    - 硬件、软件乃至产生、处理、传输、存储的各种数据或信息
- 特点
  - 没有明确的、固定的边界
  - 没有集中的控制权威。

网络空间安全

- 网络空间安全（Cyberspace Security或简称Cyber Security）：研究网络空间中的安全威胁和防护问题
  - 在有对手（adversary）的对抗环境下，研究信息在产生、传输、存储、处理的各个环节中所面临的威胁和防御措施、以及网络和系统本身的威胁和防护机制。
    - 信息的保密性、完整性和可用性
    - 网络空间基础设施的 安全和可信

网络安全形势

- 维护网络安全首次列入我国政府工作报告
  - 2014年2月27日，中央网络安全和信息化领导小组宣告成立
  - 研究制定网络安全和信息化发展战略，不断增强国家安全保障能力
  - 信息安全问题上升到国家战略层面
  - 2014年4月，中国国家安全委员会第一次会议提出总体国家安全观的概念，其中网络安全是重要组成部分
  - 2018年4月，全国网络安全和信息化工作会议，推进“网络强国”战略

“没有网络安全就没有国家安全”

网络安全形势（续）

- 各国加速网络安全战略部署
  - 美国从90年代后期开始注重关键基础设施来自网络空间的威胁，并先后制定出成熟的国家网络空间安全战略
  - 2014年2月，美国启动《网络安全框架》
  - 2017年8月18日，将美军网络司令部升级为美军第十个联合作战司令部，网络空间正式与海洋、陆地、天空和太空并列成为美军的第五战场
  - 欧洲各国合作保障升级，加强网络安全立法，以应对日益严峻的网络攻击。制定《通用数据保护条例》；建立了欧盟网络安全认证框架，加强在线服务和消费设备的网络安全
  - 日本尤其注重保障个人信息安全，大力发展网络作战能力。2018年1月，日本宣布拟设立网络和太空防卫指挥中心

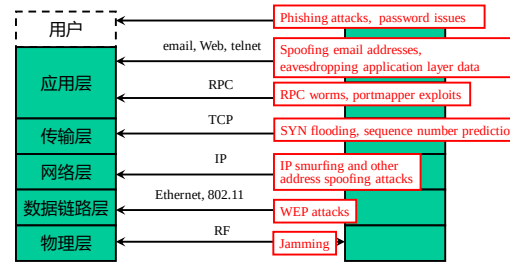
NIST发布《网络安全框架1.1》

- 美国商务部国家标准与技术研究院（简称NIST）于美国时间2018年4月16日发布《提升关键基础设施网络安全的框架》（也被称为《网络安全框架1.1》）
  - 该框架侧重于对美国国家与经济安全至关重要的行业（能源、银行、通信和国防工业等）

信息安全 vs. 网络安全 vs. 网络空间安全

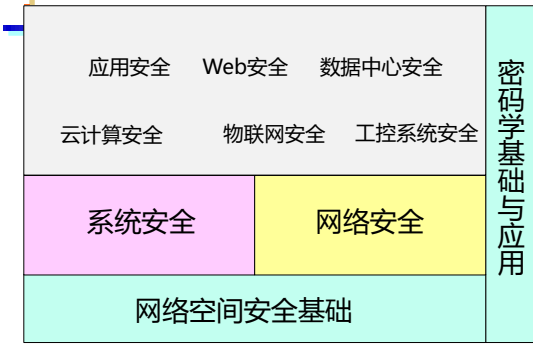
- 网络安全（Network Security）
  - 分布式网络环境中，对信息载体（处理载体、存储载体、传输载体）和信息处理、传输和存储、访问提供安全保护，以防止数据、信息内容、处理能力等被拒绝服务或被非授权使用和篡改
- 信息安全、网络安全、网络空间安全
  - 核心是信息安全问题，只是出发点和侧重点有所差别
  - 信息安全
    - 侧重于线下和线上的信息安全
  - 网络安全
    - 侧重于线上安全和网络社会安全
  - 网络空间安全
    - 侧重点是与陆、海、空、太空并列的空间概念

网络体系结构 与 网络安全



教学目标

- 理解网络空间安全体系结构的基本概念和基本原理
- 掌握计算机网络安全技术的基本原理和方法
- 掌握主流的网络攻防基础方法和技术
- 了解Internet的安全性，增强安全意识



主要内容及课时安排

网络安全基础理论

- 概述（2）
- 数据加密技术：密码学基础（4）
  - 基本概念和方法；对称密码体系；公钥密码体系
- 身份认证与密钥管理技术（2）
- 访问控制技术（2）

网络安全协议和工具

- 网络安全基础设施（12）
  - 安全协议：网络层，传输层，应用层
  - 安全防御设施：防火墙；入侵检测IDS；IPS；VPN
  - 网络攻防技术基础

系统安全和应用安全

- 系统安全和应用安全（6）
  - 恶意软件
  - Web安全
- 课堂讨论（4）

课程安排

- 本课程所需基础知识
  - 操作系统、程序设计、计算机网络等
- 授课方法
  - 课堂讲解（背景知识 + 安全主题）
  - 课外自学
  - 习题 + 小组大作业
- 课件、课程资料、作业
  - 课程中心网站 course.buaa.edu.cn
- 考核方式
  - 平时成绩：40%
    - 考勤：5%
    - 作业：35%
  - 期末考试：60%：2小时，开卷 （第16周）

参考书目

- William Stallings，网络安全基础-应用与标准（第5版），清华大学出版社，2014年5月
- William Stallings，Lawrie Brown，计算机安全原理与实践（第三版），机械工业出版社，2016年3月
- 斯坦普（Mark Stamp） 著；张戈 译，信息安全原理与实践（第2版） [Information Security: Principles and Practice, 2nd Edition]， 清华大学出版社，2013年5月
- 沈昌祥，左晓栋，网络空间安全导论，电子工业出版社，2018年4月
- Michael T. Goodrich，Roberto Tamassia, 计算机安全导论，清华大学出版社，2012年3月

大作业选题

- 确定选题
  - 不同类型题目：验证类和开发类
  - 验证类
    - 防火墙应用
    - 网络漏洞扫描
    - 无线路由器的漏洞与安全
  - 开发类
    - 基于OpenSSL的安全传输系统
    - 网络流量分析
    - 文件加解密功能实现
  - 自选题目：其他感兴趣的网络安全问题

大作业自选题目参考（往年）

- “校园网安全防范与渗透测试”
- “无线路由器漏洞与安全”
- “基于netfilter/iptables的流量限速模块”
- “基于NetfilterIPTables框架的应用层包过滤防火墙”
- “Web网站漏洞扫描”
- ……

大作业过程管理

- 分组
  - 自由组合进行分组，每组2-3人
  - 参考给定范围选择，题目自拟
- 课堂讨论
  - 小组提交开题报告并在课上汇报
  - 小组提交程序代码和ppt
- 期末提交技术报告
  - 每个学生根据大作业承担的工作提交技术报告

第一章 概述

信息安全

- 信息安全保障的需求
  - 物理方法
  - 管理方法
- 引入计算机和互联网络
  - 计算机安全
  - 网络安全
- 信息安全是一门交叉学科。
  - 广义上，信息安全涉及多方面的理论和应用知识，除了数学、通信、计算机等自然科学外，还涉及法律、心理学等社会科学
  - 狭义上，也就是通常说的信息安全，只是从自然科学的角度介绍信息安全的研究内容

计算机安全

◆美国国家标准与技术研究院（NIST）计算机安全手册的定义

❖对某个自动化信息系统的保护措施，其目的在于实现信息系统资源的*完整性、可用性和机密性*（包括硬件、软件、固件、数据/信息、电信）

"*the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications*"

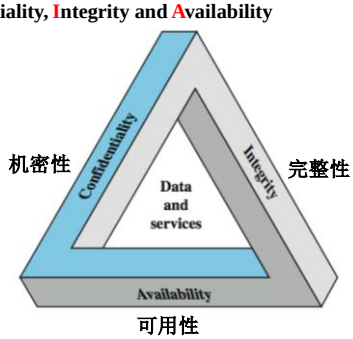
网络安全 （Network Security）

◆涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科

◆分布式网络环境中，对信息载体（处理载体、存储载体、传输载体）和信息处理、传输和存储、访问提供安全保护，以防止数据、信息内容、处理能力等被拒绝服务或被非授权使用和篡改

核心概念：CIA三元组

Confidentiality, Integrity and Availability



核心概念：CIA三元组

◆机密性Confidentiality

❖机密性是指保证信息不能被非授权访问，即使非授权用户得到信息也无法知晓信息内容，因而不能使用

➢数据机密性

➢隐私性

◆完整性Integrity

❖完整性是指维护信息的一致性，即信息在生成、传输、存储和使用过程中不应发生人为或非人为的非授权篡改。

➢数据完整性

➢系统完整性

◆可用性Availability

❖可用性是指保障信息资源随时可提供服务的能力特性，即授权用户根据需要可以随时访问所需信息

网络安全的挑战

1. 安全机制的复杂性
2. 安全机制要考虑潜在攻击和各种威胁
3. 安全机制的部署方法
4. 可信的通信协议，保护机密信息的方法
5. 攻防双方（人）的较量
6. 直到灾难发生才能察觉
7. 需要定期监控
8. 通常是事后考虑
9. 影响系统的有效性和易操作性